Policy: 8030-3- Password Authentication
Section: Computer Security
Office/Department: Information Technology

Reports To: Deputy Commissioner
Contact: 404-631-1000

PURPOSE

This document sets the IT policy to implement authentication mechanisms such as passwords to access sensitive data and the responsibility of the user to appropriately select and protect their passwords.

SCOPE

This policy applies to all GDOT Offices and Districts.

RESPONSIBILITY

1. The IT Director/CIO retains authority for enforcement and monitoring of this policy.
2. The IT Director/CIO is responsible for designating a person to serve this function in case of absence or emergency.
3. The Administrators of the IT Offices are responsible for compliance with the policy, updates to the policy, monitoring, and enforcing the policy.
4. In the absence of the IT Offices administrator, the Assistant Administrator of that particular Office is responsible for compliance with the policy and for reporting concerns to the IT Director/Chief Information Officer.

SUPPORTING DOCUMENTS

Doc ID: GTA Policy No. P-08-006.01
Title: Password Authentication
Description: Password Authentication
Effective date: 03/20/2008

Doc ID: GTA Standard No. S-08-007.01
Title: Password Authentication
Description: Password Security
Effective date: 03/31/2008

Doc ID: GTA Standard No. S-08-008.01
Title: Password Authentication
Description: Strong Password Use
Effective date: 03/31/2008

DEFINITIONS

Authentication is a process of attempting to verify the digital identity of system users or processes.

POLICY STATEMENTS

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to GDOT information systems and applications unless specifically designated as a public access resource.

All users (employees, contractors, and vendors) with access to GDOT information systems shall take the appropriate steps to select and secure their passwords.

Password Security

- All passwords shall be treated as sensitive, confidential information and shall not be shared.
- Passwords shall not be stored in clear text. Cryptography shall be used to create the stored information.
- Users shall not write passwords down or store them anywhere in their office. Nor shall they store passwords in a file on ANY computer system (including Personal Digital Assistants or similar devices) without encryption.
- All user passwords shall be changed every 30 days, or not to exceed 3 months if other documented and approved mitigating factors are in effect excluding instances such as account lockout after a number of logon attempts.
- User accounts that have system- level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
- Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
- If an account or password is suspected of being compromised, the incident must be reported to the appropriate access administrator or in accordance with Incident Response procedures.
- Temporary or "first use" passwords (e.g., new accts or guests) must be changed upon first logon the authorized user accesses the system and have a limited life of inactivity before being disabled.

Strong Password Use

- Access to all GDOT information systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher shall require the use of strong passwords or other strong authentication mechanisms.
- Strong passwords shall be constructed with the following characteristics:
    - Are at least eight characters in length
    - Must contain characters from at least three of the following four types of characters:
        - English upper case (A-Z)
        - English lower case (a-z)
        - Numbers (0-9)
        - Non-alpha special characters ($, !, %, ^, …)
    - Must not contain the user's name or part of the user's name
    - Must not contain easily accessible or guessable personal information about the user or user's family. (such as birthdays, children's names, addresses etc)

References:

***

History:

copied to GDOT Publications v.02.00.00: 02/29/12;
reviewed: 4/6/2009;
copied to P&P: 11/19/08;
created and effective 08/1808